

RECEIVED

MAR 17 2003

KEKER &amp; VAN NEST

1 WILLIAM L. ANTHONY (State Bar No. 106908)  
 2 ERIC L. WESENBERG (State Bar No. 139696)  
 3 KENNETH J. HALPERN (State Bar No. 187663)  
 4 ORRICK, HERRINGTON & SUTCLIFFE, LLP  
 5 1000 Marsh Road  
 6 Menlo Park, CA 94025  
 7 Telephone: (650) 614-7400  
 8 Facsimile: (650) 614-7401

9 STEVEN ALEXANDER (admitted *Pro Hac Vice*)  
 10 KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)  
 11 JAMES E. GERINGER (admitted *Pro Hac Vice*)  
 12 JOHN D. VANDENBERG  
 13 KLARQUIST SPARKMAN, LLP  
 14 One World Trade Center, Suite 1600  
 15 121 S.W. Salmon Street  
 16 Portland, OR 97204  
 17 Telephone: (503) 226-7391  
 18 Facsimile: (503) 228-9446

19 Attorneys for Defendant and Counterclaimant,  
 20 MICROSOFT CORPORATION

21 UNITED STATES DISTRICT COURT  
 22 NORTHERN DISTRICT OF CALIFORNIA  
 23 OAKLAND DIVISION

24 INTERTRUST TECHNOLOGIES  
 25 CORPORATION, a Delaware corporation,

26 Plaintiff,

27 v.

28 MICROSOFT CORPORATION, a  
 Washington corporation,

Defendant.

MICROSOFT CORPORATION, a  
 Washington corporation,

Counterclaimant,

v.

INTERTRUST TECHNOLOGIES  
 CORPORATION, a Delaware corporation,

Counter Claim-Defendant.

Case No. C 01-1640 SBA (MEJ)

MICROSOFT'S BRIEF IN SUPPORT  
 OF MOTION FOR SUMMARY  
 JUDGMENT THAT CERTAIN  
 "MINI-MARKMAN" CLAIMS ARE  
 INVALID FOR INDEFINITENESS

## TABLE OF CONTENTS

	Page
I. INTRODUCTION .....	1
II. FACTS .....	3
A. "Secure" Lacks a Clear Meaning in the Art .....	3
1. To Give "Secure" a Definite Meaning, a Number of Parameters Must Be Specified .....	4
a. What is to Be Protected? (Mitchell Questions 1 and 2) .....	5
b. The Properties to be Protected. (Mitchell Question 3) .....	5
c. The Threats to be Protected Against (Against Whom, What Points of Attack, What Kind of Attack.) (Mitchell Questions 4, 5, and 6) .....	6
d. The Duration and Degree of Protection. (Mitchell Questions 7 and 8) .....	7
e. How Protection is Verified and Evidenced. (Mitchell Question 9) .....	8
f. From Whose Perspective the System Is "Secure." (Mitchell Question 10) .....	8
B. The InterTrust Applicants Could Have Used the Claims or Specification to Adequately Define "Secure" But Failed to Do So .....	8
1. InterTrust Has Not Defined "Secure" in the Claims or the Specification .....	8
2. "Secure" Remains Indefinite Even When the Claim is Viewed in Light of the Specification .....	9
C. The Prosecution History Does Not Give Secure a Clear Meaning .....	11
D. Indefiniteness of Certain Patent Claims is Highlighted by Errors Made In The Specifications .....	12
1. The '683, '721 & '861 Patents Failed to Properly Incorporate the "Big Book" by Reference .....	12
2. None Of The Patents Met The "Incorporation By Reference" Requirements .....	12
E. InterTrust Failed to Fulfill Its Obligation to Define the Claim Term "Secure" as Clearly as Possible .....	12
F. InterTrust's Proposed Markman Definition Confirms That "Secure" Is Indefinite .....	13
G. Nor Is "Secure" Redeemed By The Terms It Modifies .....	14
H. InterTrust's Coined Terms "Protected Processing Environment" And "Host Processing Environment" Are Also Indefinite .....	15
1. The Terms "Protected Processing Environment" And "Host Processing Environment" Have No Ordinary Computing Art Meaning .....	15
2. The Claims Do Not Provide Substance Or Context Sufficient To Provide Meaning To Either PPE Or HPE .....	16

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

TABLE OF CONTENTS  
(continued)

	Page
3. The Specification Does Not Define The Term Protected Processing Environment.....	17
4. The Term Host Processing Environment Is Not Defined In The Specification Either.....	19
III. ARGUMENT.....	19
A. Applicable Legal Standards.....	19
1. Claim Indefiniteness Requires a Two-Part Test.....	21
2. "Secure" and Its Variants Are Indefinite Terms That Render the Claims Containing Them Invalid.....	21
B. New Or Coined Terms Must Be Defined Or Otherwise Made Clear.....	23
IV. CONCLUSION.....	24

## TABLE OF AUTHORITIES

## FEDERAL CASES

	Page
<i>Advanced Display Systems, Inc. v. Kent State University</i> , 212 F.3d 1272 .....	12
<i>Amgen, Inc. v. Chugai Pharmaceutical Co.</i> , 927 F.2d 1200, .....	21, 23
<i>Amgen Inc. v. Hoechst Marion Roussel, Inc.</i> , 314 F.3d 1313 .....	20
<i>Application of Lechene</i> , 277 F.2d 173 .....	22
<i>Ex parte Brummer</i> , 12 U.S.P.Q.2d (BNA) 1653 .....	22
<i>In re Cohn</i> , 58 C.C.P.A. 996, 438 F.2d 989 .....	21
<i>In re de Seversky</i> , 474 F.2d 671 .....	12
<i>Exxon Research and Engineering Co. v. United States</i> , 265 F.3d 1371 .....	20, 23
<i>General Electric Co. v. Wabash Appliance Corp.</i> , 304 U.S. 364, 58 S.Ct. 899 .....	23
<i>J.T. Eaton &amp; Co. v. Atlantic Paste &amp; Glue Co.</i> , 106 F.3d 1563 .....	15, 23
<i>L.A. Gear, Inc. v. Thom McAn Shoe Co.</i> , 988 F.2d 1117 .....	20
<i>Morton International, Inc. v. Cardinal Chemical Co.</i> , 5 F.3d 1464 .....	20, 21
<i>Seattle Box Company, Inc. v. Industrial Crating &amp; Packaging, Inc.</i> , 731 F.2d 818 .....	22
<i>Shatterproof Glass Corp. v. Libbey-Owens Ford Co.</i> , 758 F.2d 613 .....	21
<i>Tex. Digital System v. Telegenix, Inc.</i> , 308 F.3d 1193 .....	3
<i>Union Pacific Resources Co. v. Chesapeake Energy Corp.</i> , 236 F.3d 684 .....	9, 21
<i>United Carbon Co. v. Binney &amp; Smith Co.</i> , 317 U.S. 228 .....	20

TABLE OF CONTENTS

Page

FEDERAL STATUTES

1		
2		
3		
4	35 U.S.C. § 112, ¶ 2 .....	1, 20, 24
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 I. INTRODUCTION

2 The InterTrust patent claims' use of the vague term "secure" and its variants  
3 makes them textbook illustrations of the danger of indefinite claims. Without a definition of this  
4 malleable core term, persons of skill in the art cannot determine the scope of patent coverage.  
5 This is precisely the situation prohibited by 35 U.S.C. § 112's requirement of "particularly  
6 pointing out and distinctly claiming" the alleged invention. The purpose of the claims is to define  
7 the metes and bounds of the exclusive right that the public grants in exchange for the patentee's  
8 full disclosure. Where those boundaries are blurry, others are deterred from entering the field,  
9 allowing the patentee to exclude competition beyond the scope of the claimed invention. The  
10 InterTrust patent claims using "secure" and its variants violate the bargain with the public in this  
11 fashion, and should be found fatally indefinite and, therefore, invalid.

12 InterTrust's testifying expert concedes that "security" is an "essential aspect" of  
13 the "invention," InterTrust's so-called "Virtual Distribution Environment" ("VDE"). Declaration  
14 of Eric L. Wesenberg, Ex. A, Reiter Depo., 23:21-24:9.<sup>1</sup> "Secure," or some close derivative  
15 thereof, appears in virtually every disputed claim. Reading Claim 1 of U.S. Patent No. 5,892,891  
16 ("the '891 patent") demonstrates the extensive use of the vague term "secure":

17 A method for using at least one resource processed in a secure  
18 operating environment at a first appliance, said method  
19 comprising: securely receiving a first entity's control at said first  
20 appliance, said first entity being located remotely from said  
21 operating environment and said first appliance; securely receiving  
22 a second entity's control at said first appliance, said second entity  
23 being located remotely from said operating environment and said  
24 first appliance, said second entity being different from said first  
25 entity; and securely processing a data item at said first appliance,  
26 using at least one resource, including securely applying, at said  
27 first appliance, through use of said at least one resource said first  
28 entity's control and said second entity's control to govern use of  
said data item. (Emphases added.)

24 Ex. P, Claim 1. This claim uses four different, and five total, instances of this term or its variant.  
25 Neither the claims nor the rest of the patents define what it means for something to be "secure" or  
26 to be done "securely." "Secure," in the art, is a highly general, relative and multifaceted term

27 <sup>1</sup> Hereinafter, all cites to exhibits ("Ex.") are to exhibits attached to the Declaration of Eric L.  
28 Wesenberg in support of Microsoft's Motion for Summary Judgment that Certain "Mini-  
Markman Claims are Invalid for Indefiniteness.

1 which, without more specific definition, fails to have a clear or even useful meaning. In all their  
2 hundreds of pages of single-spaced description, the patents never clearly or consistently define  
3 "secure," nor the composite terms using secure (e.g., "secure container"), nor the related coined  
4 terms deriving from the same concept: "protected processing environment" and "host processing  
5 environment."

6 The extrinsic evidence – both testimonial and documentary, both Microsoft's and  
7 InterTrust's – is in complete agreement: "secure" corresponds to a general concept in the  
8 computer field, which lacks specific meaning and standing alone may apply to numerous specific  
9 scenarios depending on the properties to be "secured," the particular threats posed, the means  
10 used, the degree of protection needed, the perspective from which one views "security," and so  
11 on.

12 Both parties' experts have testified that "secure" can take on a definite meaning  
13 within the context of a "security policy," which defines the parameters and sets objective criteria  
14 for determining whether they have been satisfied. Computer scientists have developed a number  
15 of models for objectively evaluating the security of different systems and architectures, at least  
16 one of which is mentioned (TCSEC), but not employed, in InterTrust's '193 patent.<sup>2</sup> InterTrust  
17 could easily have defined a security policy using any of these models. Instead, it left "secure"  
18 inscrutable throughout the patents.

19 The problem is not that it's difficult to discern the true meaning of these claim  
20 terms. It is impossible. For the reasons set forth herein, Microsoft asks that the Court find the  
21 claims containing "secure" (including its variants), "protected processing environment" or "host  
22 processing environment" invalid for indefiniteness.

23 ///

24 ///

25 ///

26 <sup>2</sup> For efficiency, all references to "the specification" are to the specification of U. S. Patent No.  
27 6,253,193 ("the '193 patent") (Ex.Q). The '193 specification reproduces, nearly identically, the  
28 "big book" original application (the original 900+ page application filed in 1995). Each of the  
patents at issue herein either expressly reproduce the same text in their specifications, or attempt  
to incorporate it by reference (though not successfully, *see infra* § II. D.).

1 II. FACTS2 A. "Secure" Lacks a Clear Meaning in the Art.

3 The most pervasive indefinite term in the InterTrust patents is "secure" in all its  
4 various forms. Indeed, the provision of "security" while enabling the flexible distribution of  
5 digital information is the stated goal of the entire invention. To construe "secure," the Court must  
6 look to the ordinary meaning (if one exists) that would be attributed to the term by a person of  
7 skill in the art. *Tex. Digital Sys. v. Telegenix, Inc.*, 308 F.3d 1193, 1202 (Fed. Cir. 2002). The  
8 intrinsic and extrinsic evidence, including InterTrust's own statements and those of its expert,  
9 establish that while communicating a general or conceptual meaning, the term "secure" lacks a  
10 any precise, uniform definition to inform a person of skill in the art what it means unless a  
11 number of questions are answered. Because InterTrust never provides the needed answers, it is  
12 impossible to determine the scope of the claims.

13 "Secure memory" for instance, is no clearer a phrase than a "secure car." At first  
14 blush, one hearing the phrase "secure car" might think of a car equipped with features that make  
15 it difficult or impossible to steal, such as a club, an alarm siren, and or an ignition "kill switch."  
16 Only later in the conversation, hearing the speaker refer to bulletproof glass, shielded wheels, and  
17 reinforced doors would the listener realize that "secure" means something entirely different: The  
18 car is in fact designed to protect passengers from attack (to transport diplomats and heads of  
19 state). Even after the type of security is identified, different particular combinations of security  
20 measures will qualify the car as "secure" in the eyes of different customers. Simply referring to a  
21 car as "secure" fails to delineate the objective of that security, the type of security needed or the  
22 measures used to achieve it. Nor does the descriptor "secure" disclose the perspective from  
23 which "security" is being assessed. A parking enforcement officer might consider a booted  
24 vehicle "secure" (i.e., from removal by its owner), while the owner might view it as "insecure"  
25 since it allowed someone to tamper with its wheels. Another variable might be the length of time  
26 the car would have to withstand the measures it is designed to resist. From this simple metaphor,  
27 the relative, multifaceted and undefined character of "secure" is readily apparent.



What is true in the vernacular applies with even greater force in the computing arts – “secure” needs definition along multiple axes to have a precise meaning. Deponents skilled and experienced in the field have spoken on this point. InterTrust’s own expert, Dr. Michael Reiter, testified that “‘secure’ is a fairly general term that’s used in the art for – in several different ways.” Ex. A, Reiter Depo., at 30:11-19. Asked to describe them, Dr. Reiter responded, “Oh, my gosh. All the ways. I can enumerate several ways I can think of on the fly. I don’t know that I can enumerate everything I would do if I had more time.” *Id.* at 31:10-17. Microsoft’s expert, Prof. John Mitchell, agrees, identifying ten different variables (discussed below) that must be known to determine what is meant by “secure.” Declaration of John Mitchell in Support of Microsoft’s Motion Summary Judgment that Certain “Mini-Markman” Claims are Invalid for Indefiniteness (“Mitchell Decl.”) at 8-11. Others involved in this industry, including some who have done, or do, business with InterTrust have testified to similar effect:

- MusicMatch; stated that in order to know whether a system is secure, one would have to know what the content provider for that system intended, and thus “security” as it applies to a particular system might mean something completely different from the same term applied to a different system. Ex. C, Jim McLaughlin Depo., p. 55:14-25.
  - Envivio; stated that “secure” “doesn’t mean anything in general. It means a general concept.” Ex. D, Julien Signes Depo., at 40:22-41:2. When asked whether “it would be necessary ... to look at the context of the implementation of ... security to understand whether or not a system is secure,” Mr. Signes answered, “yes, of course.” *Id.* at 41:3-13.
  - A leading authority in the field has written that “[w]ithout a precise definition of what security means and how a computer can behave, it is meaningless to ask whether a particular computer system is secure.” Ex. E, Carl E. Landwehr, “Formal Models for Computer Security,” ACM Computing Surveys, v.13 no. 3 (1981).
  - “When someone states that ‘My computer is secure,’ that statement may very well mean distinctly different things to different people.” Ex. F, Taylor, *Comparison Paper Between the Bell and LaPadula Model and the SRI Model*, IEEE Symp. on Security & Privacy, 1984, pg. 195, 197.
1. To Give “Secure” a Definite Meaning, a Number of Parameters Must Be Specified.

John Mitchell, a Professor of Computer Science at Stanford University, has identified ten parameters that persons of skill in the art would need to know in order to have a shared understanding of the meaning of “secure” in any given instance: (1) what types of things

1 or actions are protected; (2) what specific things or actions are protected in the system in  
2 question; (3) what properties of those things are protected; (4) against whom; (5) against what  
3 points of attack; (6) against what kind of attack; (7) for how long; (8) to what degree of  
4 protection; (9) how is protection or the loss thereof evidenced; and (10) the perspective (or  
5 perspectives) from which "security" should be considered. Mitchell Decl., 8-11 and *passim*. To  
6 be able to evaluate whether an actual system is "secure," people of skill in the art must first reach  
7 a common understanding of each of these variables, as discussed below.

8 a. What is to Be Protected?  
9 (Mitchell Questions 1 and 2)

10 The first variable is, what is being protected? See Mitchell Decl., at 9. Is the user  
11 being protected from untrusted data, or is data being protected from untrusted users? *Id.* How  
12 "secure" is understood by people of skill in the art is influenced in the first instance by what one  
13 is trying to protect, and here the claims force them to guess. InterTrust has at least partly  
14 admitted that this is true. InterTrust objected to answering a Request for Admission that "a  
15 password-protected file is secure," on the ground that it was not told, *inter alia*, "the value of the  
16 information in the file." See Ex. G, InterTrust's Response to Microsoft Request for Admission  
17 101. In InterTrust's view, in other words, the presence or absence of "security" depends on the  
18 nature of the thing to be protected. For a high-value item, a password requirement alone might  
19 not be enough to make the item "secure," while the same barrier might suffice to ensure the  
20 "security" of a low-value item.

21 b. The Properties to be Protected.  
22 (Mitchell Question 3)

23 The next crucial component of security is which attributes of the protected items  
24 are safeguarded. The different properties include:

- 25 • secrecy (or, "confidentiality") – maintaining the secrecy of data so that its  
26 meaning is not learned by unauthorized parties;
- 27 • integrity – ensuring that data may not be altered or destroyed by  
28 unauthorized parties;
- availability – ensuring that authorized parties can use the computers'

1 systems and data when desired;

- 2 • authenticity – ensuring accurate proof of the identity (or perhaps other characteristics) of the author or sender of a message or data;
- 3 • non-repudiation – preventing denial of the origination or receipt of messages by parties.

4 Mitchell Decl., 9-10. AOL and MusicMatch agree that security includes one or more of these  
5 components. AOL; Ex. H, Saccocio Depo., 30:8-31:16 (confidentiality, integrity, non-  
6 refutability, authentication); MusicMatch; Ex. C, McLaughlin Depo., 34:16-35:14 (integrity,  
7 authentication, non-repudiation, but not necessarily secrecy). So does InterTrust's expert, who  
8 testified that "secure" could be defined narrowly to include a single criterion, "secrecy," or in  
9 contrast, requiring satisfaction of the "Common Criteria," a multi-criteria framework for  
10 identifying security requirements and evaluating systems and whether they meet those  
11 requirements. Ex. A, Reiter Depo., 31:22-25, 32:15-20; Mitchell Decl., at 7, n. 1 (*see also*  
12 <http://www.commoncriteria.org>). Any one of these features alone, or any combination of them  
13 might suffice to create a "secure" system, depending on the context. The assurance of  
14 "availability" might be integral to the meaning of "secure" for one user, but not for another user  
15 with different priorities, as Dr. Reiter testified:  
16

17 Q: How about availability of information? Are you familiar  
18 with the concept of availability in...

19 A. Sure, sure.

20 Q. Are there some senses of the word secure where ensuring  
21 availability is required and other senses of the word secure  
22 where ensuring availability is not required?

23 A. Yes, I'd say that's true.

24 Ex. A, Reiter Depo., 36:9-18 (objections and other non-substantive matter omitted).

25 c. The Threats to be Protected Against (Against Whom, What  
26 Points of Attack, What Kind of Attack.)  
(Mitchell Questions 4, 5, and 6)

27 Further crucial variables in defining "secure" are the types of attackers, the  
28 different possible points of attack, and the types of threats posed. Mitchell Decl., at 10. A system  
billed as "secure" against attack by outsiders might not be "secure" for a customer requiring a

1 system that even insiders cannot misuse, or for a customer who requires protection not against its  
 2 own employees but against a category of outsiders possessing certain identified information about  
 3 the system or other special resources. See, e.g. Mitchell Decl., at 10, 20, 31, 34 (regarding  
 4 "secure memory" "secure container," "secure operating environment" etc.).

5 The types of threats one has in mind are essential to defining "secure." As  
 6 InterTrust itself argued in response to Microsoft Request for Admission that "a password-  
 7 protected file is secure," one must know, *inter alia*, "the threats against which the file is to be  
 8 protected." See Ex. G, InterTrust's Response to Microsoft Request for Admission 101.  
 9 InterTrust's expert echoed this view, testifying that:

10 "secure" is used as a general term to refer to protection against  
 11 misuse and interference, and to truly evaluate that security, you  
 12 often need to be more precise about the sorts of misuse and  
 13 interference you are concerned with, the threat models or the  
 14 threats to which a system or primitive is likely to be subjected,  
 15 and the mechanism by which you protect that system.

16 Ex. A, Reiter Depo., 33:17-34:5 (emphasis added).

17 d. The Duration and Degree of Protection.  
 18 (Mitchell Questions 7 and 8)

19 The duration and degree of protection are also prerequisites to understanding the  
 20 meaning of "secure" in the art. Mitchell Decl., at 10-11. Withstanding an hour-long attack, or an  
 21 attack employing a certain level of computing power might be sufficient in one context, but not  
 22 another. Mitchell Decl., at 10. As to degree of protection, America Online's Director of Rich  
 23 Media agreed that some notion of degree is needed to understand "secure":

24 Q: But they [the criteria for "security"] can be met sufficient so  
 25 that it's meaningful within this industry to use the term  
 26 "secure," can they not?

27 A: It's a vague term. I know it's frustrating, but it is. Security  
 28 is a vague term. How much security is a better question.

Ex. H, Deposition of Damian Saccocio, 40:12-17.

///

///

e. How Protection is Verified and Evidenced.  
(Mitchell Question 9)

"Security" also depends on the manner in which continued protection, or the loss thereof, is or is not measured, tested, proven or evidenced analytically. Mitchell Decl., 11.

f. From Whose Perspective the System Is "Secure."  
(Mitchell Question 10)

Finally, the perspective from which "security" is viewed is crucial. A system can be "secure," or not, to a content owner, the system administrator, and or the authorized users. Mitchell Decl., at 11. Take for example, the case of a user who downloads a music file for a fee, which she pays electronically, using her credit card. If a third party tries to intercept the credit card information and make an additional, free copy of the downloaded file for himself, different outcomes could be viewed as "secure" by the different parties to the transaction. If the third party successfully copies the file, but not the credit card information, then the system might be considered "secure" from the perspective of the customer, but not the vendor. If, on the other hand, the attacker fails to copy the file, but does obtain the credit card information, and the system merely detects the unauthorized intrusion, then the vendor might consider the system "secure" while, from the customer's perspective, it is "insecure" – or at least the customer will see it that way, if she later learns of the theft.

B. The InterTrust Applicants Could Have Used the Claims or Specification to Adequately Define "Secure" But Failed to Do So.

1. InterTrust Has Not Defined "Secure" in the Claims or the Specification.

InterTrust could have chosen to define the term "secure" but didn't. Ten of the twelve claims at issue employ the word "secure" in some form, yet none of them defines it. Ex. J, JCCS Ex. H. They establish no security policy and no criteria that would answer the ten questions discussed above.

///

///

///

2. "Secure" Remains Indefinite Even When the Claim is Viewed in Light of the Specification.

Though "secure," and its variants, as used in the claims, lack requisite definiteness, the claims could still be saved from indefiniteness if "those skilled in the art would understand the scope of the claim when the claim is read in light of the rest of the specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir. 2001). Far from curing the problem, however, the patent specification compounds it. It contains no uniform security policy, no uniform criteria for security, and no glossary. It uses "secure" and "security" in multiple, vague and inconsistent senses, giving the potential entrant into the field no more clarity than do the claims alone.

a) The Specification Describes Multiple Perspectives from which "Secure" Might Be Measured, and Indexes "Secure" to the Unpredictable Needs of Different Users

The specification uses "secure" in a fashion that is impossible for a person of skill in the art to understand because it depends on the unpredictable and varying needs of potential customers. In other words, "secure" cannot be defined completely by looking at the patent documents in light of the art. Instead, the '193 specification (Ex. Q) defines "secure" in terms of whatever the market may be seeking, which changes over time and has no fixed technological meaning:

- The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. ('193 at 49:59-62)
- "a "sufficiently" secure (for the intended applications) environment" ('193 at 45:23-24)
- "with sufficient security (sufficiently trusted) for the intended commercial purposes" ('193 at 45:43-45)
- Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. ('193 at 15:67-16:5).

b) The Specification Mentions Different and Inconsistent Secure Properties

The specification suggests several different security properties denoted by "secure" without committing to any of them. For example, "secure" could mean that an item or process is simply encrypted ('193 at 126:6-7), or "encrypted and tagged" (*id.* at 22:18-19), or "encrypted and authenticated" (*id.* at 45:39-40), or not encrypted but "otherwise secured ... such as by employing authentication and/or error-correction" (*id.* at 63:37-39).

c) The Specification Mentions Many Different and Inconsistent Degrees of Security

The specification uses at least a dozen adjectives apparently identifying different "levels" of security – truly secure ('193 at 80:31, 81:14, 88:38); extremely secure ('193 at 67:21); highly secure ('193 at 22:16, 23:49, 36:9-10, 41:34, 67:19, 77:30, 104:63, 132:63, 203:66, 232:47, 233:4); commercially secure ('193 at 2:20, 47:6); adequately secure ('193 at 12:50); acceptably secure ('193 at 129:25); sufficiently secure ('193 at 9:12, 16:25, 21:48, 28:47, 49:41, 207:20, 249:51); appropriately secure ('193 at 77:16); physically secure ('193 at 13:20); sufficiently physically secure ('193 at 13:20); cryptographically secure ('193 at 202:44); continually secure ('193 at 32:4); relatively secure ('193 at 63:66); non-secure ('193 at 26:22, 49:10, 62:44, 73:56, 78:16, 77:43, 80:13, 80:20, 81:19, 120:38, 139:59, 229:20); possibly less secure ('193 at 80:33).

Though the meaning of these different degrees of security is unclear, it is evident that the degree of security, like the type of security, is a function of unpredictable factors in the marketplace outside the "world" of the patent. For instance, the patent claims that "[d]irect attack on these [cryptographic] algorithms is assumed to be beyond the capabilities of an attacker. For domestic versions of VDE 100 some of this is probably a safe assumption since the basic building blocks for control information have sufficiently long keys and are sufficiently proven." '193 at 221:12-17. But what was "sufficiently long" in 1995 may not be sufficiently long now or five years from now – that is a function of changes in the larger security environment. Elsewhere, the specification promises that "the VDE 100 provided by the preferred embodiment has sufficient

1 security to help ensure that it cannot be compromised short of a successful 'brute force attack,'  
 2 and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any  
 3 value to be derived." Ex. Q, '193 at 199:38-47. But the relationship between the cost of a "brute  
 4 force attack" (essentially an attack that tries all possible keys no matter how long it takes) and the  
 5 "value to be derived" by cracking a given system depends on the characteristics of the parties  
 6 involved and changes in technology, which are "outside" the patent. The patent describes  
 7 "secure" not in terms of technological means but in terms of ever-changing marketplace factors.

8 d) **The Specification Mentions Different and Inconsistent Security**  
 9 **Methods**

10 Throughout the patent, different measures are described as possibly sufficient for  
 11 security, but no indication is given of which measures are necessary to security:

- 12 • "a secure enclosure, such as a tamper resistant metal container or some form of  
 13 a chip pack containing multiple integrated circuit components" ('193 at 169:7-  
 10)
- 14 • "In one example, tamper resistant security barrier 502 is formed by security  
 15 features such as "encryption," and hardware that detects tampering and/or  
 destroys sensitive information" ('193 at 59:55-58)

16 The attached declaration of Professor John Mitchell provides many more examples of the vague,  
 17 multiple and inconsistent uses of "secure" and its variants in the patent specification. Mitchell  
 18 Decl. at 12-17.

19 C. **The Prosecution History Does Not Give Secure a Clear Meaning.**

20 There is nothing in the prosecution history of any of the seven patents that resolves  
 21 any of the problems discussed above. The prosecution histories do not offer any definition,  
 22 criteria, or aid of any kind to help one of skill in the art understand what is meant by the term  
 23 "secure" and its variants in the claims. Moreover, to the extent the continuation-in-part patents  
 24 criticize the "big book" application as NOT teaching how to defend against a given threat (for  
 25 example, "bogus load modules" that can "wreak havoc," (Ex. R, U.S. Patent No. 6,157,721  
 26 ("721") '721 at 7:37, 8:16)), they raise even more questions about what "secure" could possibly  
 27 mean in these claims.  
 28



1 D. Indefiniteness of Certain Patent Claims is Highlighted by Errors Made In  
2 The Specifications

3 1. The '683, '721 & '861 Patents Failed to Properly Incorporate the "Big  
4 Book" by Reference

5 An outside publication can be made part of a patent by referring to it, rather than  
6 actually reproducing its text. See *In re de Seversky*, 474 F.2d 671 (C.C.P.A. 1973). Whether  
7 material has been "incorporated by reference" is a question of law. *Advanced Display Systems,*  
8 *Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). "Essential" material (i.e.,  
9 that which is necessary to describe the claimed invention) may only be incorporated by reference  
10 to an issued U.S. Patent or a published U.S. Patent Application. This requirement eases the  
11 burden on the public reviewing the patent, as it makes essential material readily available,  
12 whereas non-published material, like patent applications may not be available, or must be ordered  
13 at a considerable expense from the patent office. See e.g., MPEP § 608.01 (p).

14 "The big book" material is "essential" in U.S. Patent No. 6,185,683 ("'683")  
15 (Ex. S) the '721, and U.S. Patent No. 5,920,861 ("'861") (Ex. V). In each of the patents, the "big  
16 book" is relied on to explain fundamental portions of the claimed inventions. See '721 at 4:51-  
60; '861 at 2:37-39; and '683 at 27:1-16.

17 2. None Of The Patents Met The "Incorporation By Reference"  
18 Requirements

19 The '683, '721, and '861 patents all purport to incorporate the "big book" by  
20 reference to the unpublished patent *application*. '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11.  
21 They never amended their specifications to properly reference the issued patent number. This  
22 failure means that the "big book" materials are not part of the '721, '683 or '861 patents.  
23 Therefore, any need for definitions therefrom renders the claims and patents indefinite and  
24 invalid.

25 E. InterTrust Failed to Fulfill Its Obligation to Define the Claim Term "Secure"  
26 as Clearly as Possible

27 The extrinsic evidence, including InterTrust's own documents, indicates that it had  
28 the opportunity to be more precise. In this regard, InterTrust not only failed to apprise what the

1 bounds of the claim were, but also failed to be as precise as the subject matter permits. It is  
 2 implicit in the lengthy discussion of parameters above that the term "secure" can be used with  
 3 clear meaning in this field only after all the questions are answered. Typically this takes the form  
 4 of a "security policy" and "criteria" for measuring satisfaction of that policy. A "security policy"  
 5 answers "secure for whom?" and "secure for what purposes?" The security policy defines what is  
 6 being protected against what attacks or threats (questions 1-6 of Mitchell Decl.). "Criteria" are  
 7 designated as objective measurements for determining whether a real system satisfies the security  
 8 policy. (Questions 7-10 of Mitchell). Together, the security policy and criteria allow the word  
 9 "secure," which otherwise is a general and merely conceptual term, to be used in a meaningful  
 10 and definite manner. The InterTrust patent claims and specification contain no uniform security  
 11 policy, and no uniform definition of "secure."

12 The need for a specific security policy and criteria is well known in the field:

13 "A given system can only be said to be secure with respect to its  
 14 enforcement of some specific policy." Ex. L, *Trusted Computer  
 System Evaluation Criteria* (1985), pg. 59.

15 See also Ex. M, Landwehr, Carl E. *How far can you trust a*  
 16 *computer?*, SAFECOMP'93, Proc. of the 12th International Conf.  
 17 on Compute Safety, Reliability, and Security, Poznan-Kiekrz,  
 Poland, Oct., 1993, Janusz Gorski, ed., ISBN 0-387-19838-5,  
 Springer-Verlag, New York, 1993.

18 As quoted above, InterTrust's expert, Dr. Reiter, affirmed the need to establish criteria to evaluate  
 19 whether a real-world system is or is not, secure,<sup>3</sup> and recognized the role of a security policy in  
 20 providing such criteria:

21 [I]f a system has been evaluated via the common criteria, for  
 22 example, to a given protection profile, this would be an example.  
 23 You know, someone might say that it's secure once it's been  
 evaluated via that framework. Ex. A, Reiter at 32:15-20.

24 F. InterTrust's Proposed Markman Definition Confirms That "Secure" Is  
Indefinite.

25 Although the claim construction stage of litigation is far too late to cure patent

26 "[S]ecure' is used as a general term to refer protection against misuse and interference, and to  
 27 truly evaluate that security, you often need to be more precise about the sorts of misuse and  
 28 interference you are concerned with, the threat models or the threats to which a system or  
 primitive is likely to be subjected, and the mechanism by which you protect that system." Ex. A,  
 Reiter at 33:23-34:5.

1 indefiniteness, it is telling that InterTrust did not even try to clarify the term. On the contrary,  
2 InterTrust's proposed definition of "secure" confirms its utter vagueness. InterTrust asserts that  
3 "secure" means that "[o]ne or more mechanisms are employed to ... discourage misuse of or  
4 interference with information..." and can be achieved through "tamper resistance," elsewhere  
5 defined merely as "making tampering more difficult and/or allowing detection of tampering."  
6 Joint Claim Construction Statement filed in this Court on March 14, 2003. At the same time,  
7 InterTrust proposes that "[s]ecurity is not absolute, but is designed to be sufficient for a particular  
8 purpose." Joint Claim Construction Statement, at 6. Defining a claim relative to an unspecified  
9 "particular purpose" gives rise to precisely the uncertainty that Section 112(2) seeks to avoid.  
10 Moreover, whose perspective is sufficiency to be determined from and how are the "particular  
11 purposes" of the different users to be identified? By proposing a definition of "secure" that leads  
12 to inconsistent results, depending, for example, on who gets to specify a product's purpose, or  
13 whether its design is sufficient, InterTrust's own proposed definition confirms that the term has  
14 no definite meaning.

15 **G. Nor Is "Secure" Redeemed By The Terms It Modifies.**

16 None of the following claim phrases has a commonly shared understanding or  
17 usage in the field: "secure operating environment," "secure container," "secure memory," "secure  
18 database," "secure execution space," "securely applying," "securely assembling," "securely  
19 processing," or "securely receiving." Mitchell Decl., at 19-51. None of these terms resembles  
20 "smart card" or "hot dog," terms in which otherwise vague and subjective adjectives are made  
21 clear by that which they modify. In contrast, "secure" as it appears in the claims receives no  
22 assistance from the terms it modifies. A person of ordinary skill in the art would have to have  
23 answers to the questions discussed above to know in what sense each of these items is "secure."  
24 Intertrust's expert, Dr. Reiter, acknowledged that describing an item as "secure" does not, for  
25 instance, apprise one of whether it is protected against, say, denial of service attacks or attacks on  
26 causal logic, or whether the availability of information is ensured, to name just a few aspects of  
27 the concept. Ex. A, Reiter Depo., at 30-32; Mitchell Decl., at 6-7.

28 The problem with these compound terms is made intractable with InterTrust's

1 argument that "secure" must have the same meaning everywhere it appears. In its *Markman*  
2 statement, InterTrust proposed defining "secure" independently for *Markman* purposes, and  
3 defining all other claim terms that incorporate it by reference to "secure". Thus, for "secure  
4 container," InterTrust proposes the definition, "a container that is Secure." See e.g., JCCS, Ex. B.  
5 "Secure database," "secure execution space," "secure memory," and "secure operating  
6 environment" are all to be defined in analogous fashion. *Id.* Within InterTrust's proposed  
7 definitions of the phrases "securely applying," "securely assembling," "securely processing," and  
8 "securely receiving," the word "securely" is defined simply as "in a Secure manner." *Id.*  
9 InterTrust has bound itself to the position that all of these phrases must share a common  
10 definition of "secure." All claims containing that term, then, are indefinite and invalid.

11 H. INTERTRUST'S COINED TERMS "PROTECTED PROCESSING  
12 ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" ARE  
13 ALSO INDEFINITE.

13 In its patents, InterTrust introduces the terms "Protected Processing Environment"  
14 (or "PPE") and "Host Processing Environment" (or "HPE") — InterTrust coined these terms.  
15 Recognizing that they were new, proprietary terms, InterTrust often provides initial capitalization  
16 to the phrases or sets them off by quotation marks within the specification. (See, e.g. Ex. Q, '193  
17 at 9:29, 13:10, 50:40, 105:18-19, 283:46). These coined terms also appear in several claims  
18 including some of the mini-*Markman* claims (e.g. Ex. S, the '683 claim 2, and Ex. R, '721 claim  
19 34.) It is the patentee's "duty to provide a precise definition" of terms unknown to those of  
20 ordinary skill in the art. *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1570  
21 (Fed. Cir. 1997).

22 1. THE TERMS "PROTECTED PROCESSING ENVIRONMENT"  
23 AND "HOST PROCESSING ENVIRONMENT" HAVE NO  
24 ORDINARY COMPUTING ART MEANING.

24 The terms "Protected Processing Environment" ("PPE") and "Host Processing  
25 Environment" ("HPE") do not have an ordinary or customary meaning inside or outside of the  
26 computing world. They have not been found in any dictionaries that Microsoft has consulted.  
27 InterTrust has offered no dictionary or other extrinsic references to provide a meaning for these  
28 terms.

1 Significantly, even InterTrust's testifying expert confirmed that the terms would  
 2 not have a known meaning to one of ordinary skill in the art in February 1995, when InterTrust  
 3 submitted the "big book" application. Regarding the term "Protected Processing Environment,"  
 4 Dr. Reiter testified:

5 Q. ...in February 1995, would the person of ordinary skill in the  
 6 art have heard of the phrase protected processing  
 environment?

7 A. It's not a term in the art. One might assume certain things  
 8 about that, but it's not a term in the Art.

9 (Ex. A, Reiter Depo., 131:22-132:2). He testified similarly that a person of ordinary skill would  
 10 not be familiar with the term HPE. *Id.* at 132:3-6.

11 Not surprisingly, third party deponents, all of which had close dealings with  
 12 InterTrust (most licensees of the asserted patents) were at a loss to assign any meaning, ordinary  
 13 or otherwise, to these terms. See Ex. D, Envivio Depo. at 53:9-19 ("Q: Have you ever heard the  
 14 term "protected processing environment"? A: No."); Ex. H, AOL Depo at 82:21-92:3; 96:4-  
 15 97:17.

16 2. THE CLAIMS DO NOT PROVIDE SUBSTANCE OR CONTEXT  
SUFFICIENT TO PROVIDE MEANING TO EITHER PPE OR HPE.

17 These coined terms are used in three of the "Mini-Markman" claims: PPE is  
 18 found in two and HPE is found in one. The claims do not provide the necessary context to  
 19 formulate a sufficiently definite meaning.

20 The words of Claim 2 of the '193 patent, provide little information about what is  
 21 meant by PPE. While it does partially indicate what is being protected, "*in part protecting*  
 22 *information contained*", from what, "*from tampering*" and by who, "*by a user*", it still fails to  
 23 inform one of ordinary skill if it "protects" "part" of the information or is "part" of the  
 24 "protection". Also left open is what partial protection from tampering means. Does it merely  
 25 detect that tampering has occurred, does it prevent tampering entirely or does it simply make  
 26 tampering more difficult to achieve. It is impossible to divine from the claim language itself what  
 27 is being claimed. As to its structure, the claim language recites merely that "said protected  
 28 processing environment including hardware or software."

1 Other deficiencies can be seen in Claim 34 of the '721 patent. There, the open-  
2 ended identification of PPE as "comprising: a first tamper resistant barrier" which itself has a  
3 "first security level," a "first secure execution space," and "at least one arrangement" which  
4 prevents an identified operation. Conspicuously, this description relies on "secure" and  
5 "security." For the reasons noted above, this claim language lends no clarity to PPE but  
6 compounds its indefiniteness. Furthermore, one of ordinary skill cannot identify what is being  
7 "protected." See Mitchell Decl. at 35-37.

8 In Claim 155 of the '900 patent (Ex. T) InterTrust introduces another coined term  
9 "Host Processing Environment" (HPE). While Claim 155 attempts to provide an elaboration of  
10 what is meant by HPE through the use of the term "comprising," the description which followed  
11 only serves to obscure the meaning and scope of this new term.

12 While one of ordinary skill in the art reading Claim 155 could surmise that the  
13 HPE has at least a central processing unit, main memory and "mass storage," beyond this, the  
14 scope and reach of this term is indefinite. The claim goes on to assert that the "mass storage" of  
15 the HPE stores "tamper resistant software." This passage fails to set forth with meaningful clarity  
16 whether the tamper resistant software is an aspect of the Host Processing Environment. The base  
17 description of what *might* be parts of an HPE is insufficient to inform one of ordinary skill in this  
18 art as to what the meaningful boundaries and scope of this claim limitation are.

19 3. THE SPECIFICATION DOES NOT DEFINE THE TERM  
20 PROTECTED PROCESSING ENVIRONMENT.

21 Lacking a context or definition in the claims, the specification must be reviewed  
22 for guidance as to the term's meaning. The specification fails as well. InterTrust's first use of the  
23 term PPE in the '193 specification states merely that it is one component in a preferred  
24 embodiment of a VDE "secure subsystem." Ex. Q, '193 at 9:28. This provides neither  
25 information about, nor explanation of, what a PPE is or does. General reference is then made to  
26 the PPE in the "Brief Description of the Drawings" but no meaningful discussion, and certainly  
27 no definition is provided. '193 at 50:39-41. PPE is not again revisited until Col. 79, ln. 34. Here  
28 the patent states that a Host Event Processing Environment (HPE) 655 and Secure Event

1 Processing Environment (SPE) 503 "may be generically referred to as 'Protected Processing  
2 Environments' 650". In Column 105 (at ln. 17-22), the specification states simply that hereinafter  
3 in the specification, "unless context indicates otherwise, references to any of 'PPE 650,' 'HPE  
4 655' and 'SPE 503' may refer to each of them." There is no substantive discussion of PPE after  
5 this entry.

6 InterTrust's treatment of PPE is fatally defective for multiple reasons. First, while  
7 being a coined term which refers to a feature central to InterTrust's VDE world (i.e., "the  
8 invention"), it is never clearly described. At best, InterTrust attempts to give examples of what  
9 the "generic" usage of PPE might refer to. Both Secure Event Processing Environments (SPE)  
10 and Host Event Processing Environments (HPE) are "environments" which "may be generically  
11 referred to as 'Protected Processing Environments' 650". '193 at 79:30-35. In the first instance,  
12 InterTrust attempts to illuminate the meaning of a coined term with other coined terms, an  
13 unhelpful exercise. As InterTrust's expert identified, SPE and HPE are themselves terms which  
14 would not have been known to one of ordinary skill in the art in February 1995.

15 Q. Okay. In February 1995, would the person of ordinary skill  
16 in the art have been familiar with the term host processing  
environment?

17 A. I think not.

18 Q. In February of 1995, would the person of ordinary skill in  
19 the art have been familiar with the phrase secure processing  
environment?

20 A. So I have trouble putting my finger on specific usages of  
21 that of those three words that I would say were  
commonplace, but perhaps like protected processing  
22 environment, one might—who saw that might assume  
certain things, but—so I guess my answer would be no, it  
23 wasn't a well defined term in the field at the time, but put  
together they kind of make sense.

24 Ex. A, Reiter Depo., 134:6-16. Furthermore, there are marked differences between a HPE and  
25 SPE rendering the "generic class" to which PPE refers undefined. See Mitchell Decl. at 51-53.

26 To compound the confusion, in many instances where a feature or component of a  
27 PPE is set forth, it is qualified with the term "may" indicating that the described feature is  
28 optional, hence, may or may not be a part of PPE. This practice further obscures the inherently

1 ambiguous nature of coined terms. For example, "Protected Processing Environment may refer  
2 generally to SPE and/or HPE . . ." (Ex. Q, '93 at 105:18-21). This invariably leaves the relevant  
3 public guessing at what might infringe. Such an unconstrained explanation fails to provide  
4 sufficient precision.

5 4. THE TERM HOST PROCESSING ENVIRONMENT IS NOT  
6 DEFINED IN THE SPECIFICATION EITHER.

7 The specification of the '900 patent (Ex. T) does not clear up what the claims  
8 leave vague. "Host processing environment" appears initially in the '900 specification in Col. 12  
9 where it is identified that in "some embodiments" certain functions described in the specifications  
10 "may be performed by software, for example, in host processing environments of electronic  
11 appliances" Ex. T, '900 at 12:27-29 (emphasis added). This introductory use of the term "host  
12 processing environment" sheds no light on what it is, what it does or what its parameters are. The  
13 term is first used with all initial caps, indicating its coined nature, in Col. 3 at ln. 7, with no  
14 accompanying elaboration or definition. Aside from a passing reference in Col. 13, the term is  
15 not seen again until Col. 84, ln. 39 where it appears in the simple statement that "another instance  
16 of ROS [Rights Operating System] 602 might perform the same task using a *host processing*  
17 *environment* running in protected memory that is emulating a SPU in software." Again, this  
18 section of the specification does not elaborate on what the details or constituents of a "host  
19 processing environment" are.

20 As mentioned above with regards to "protected processing environment," the  
21 specifications suggest that "host processing environment," "protected processing environment"  
22 and "secure processing environment" are terms used as synonyms or as subsets of the other. The  
23 mingling of definitions of these coined phrases further aggravates the inherent ambiguity of their  
24 use in these patents.

25 III. ARGUMENT

26 A. Applicable Legal Standards

27 The patent statute requires that every patent include "one or more *claims*  
28 *particularly pointing out and distinctly claiming* the subject matter which the applicant regards



1 as his invention." 35 U.S.C. § 112, ¶2 (emphasis added). Patent claims that fail to provide such  
2 fair warning are invalid. *Morton Int'l, Inc. v. Cardinal Chem. Co.*, 5 F.3d 1464, 1470 (Fed. Cir.  
3 1993) (affirming holding of patent invalidity because "the claims at issue [were] not sufficiently  
4 precise to permit a potential competitor to determine whether or not he is infringing"). The  
5 Supreme Court explained the "definiteness" requirement and the "chilling" effect that indefinite  
6 patents have on legitimate competition as follows:

7 The statutory requirement of particularity and distinctness in claims  
8 is met only when they clearly distinguish what is claimed from  
9 what went before in the art and clearly circumscribe what is  
10 foreclosed from future enterprise. A zone of uncertainty which  
enterprise and experimentation may enter only at the risk of  
infringement claims would discourage invention only a little less  
than unequivocal foreclosure of the field.

11 *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228, 236 (1942). Without abandoning that  
12 important principle, the Federal Circuit has made clear that "we have not held that a claim is  
13 indefinite merely because it poses a difficult issue of claim construction." *Exxon Research and*  
14 *Eng'g Co. v. United States*, 265 F.3d 1371, 1375 (Fed. Cir. 2001). Summarizing its requirements,  
15 the *Exxon* court stated:

16 ... what we have asked is that the claims be amenable to  
17 construction, however difficult that task may be. If a claim is  
18 insolubly ambiguous, and no narrowing construction can properly  
19 be adopted, we have held the claim indefinite... By finding claims  
20 indefinite only if reasonable efforts at claim construction prove  
futile, we accord respect to the statutory presumption of patent  
validity (citation omitted) and we protect the inventive contribution  
of patentees, even when the drafting of their patents has been less  
than ideal.

21 *Id.* Indefiniteness must be shown by clear and convincing evidence. *L.A. Gear, Inc. v. Thom*  
22 *McAn Shoe Co.*, 988 F.2d 1117 (Fed. Cir. 1993). "The standard of indefiniteness is somewhat  
23 high; a claim is not indefinite merely because its scope is not ascertainable from the face of the  
24 claims." *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1342 (Fed. Cir. 2003).  
25 While the standard is high, "compliance with the written description requirement is essentially a  
26 fact-based inquiry that will "necessarily vary depending on the nature of the invention claimed."  
27 Quoting *Enzo Biochem v. Gen-Probe, Inc.*, 296 F.3d 1316, 1324 (Fed. Cir. 2002) (internal  
28 citation omitted). *Id.* at 1330 (affirming finding of indefiniteness). Further, "it is not [the court's]

1 function to rewrite claims to preserve their validity." *Allen Eng'g Corp. v. Bartell Indus.*, 299  
2 F.3d 1336, 1349 (Fed. Cir. 2002).

3 1. Claim Indefiniteness Requires a Two-Part Test

4 The test for determining whether a claim is definite is "whether those skilled in the  
5 art would understand the scope of the claim when the claim is read in light of the rest of the  
6 specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir.  
7 2001); *Morton*, 5 F.3d at 1470. The Federal Circuit has identified two parts to this test: 1) the  
8 patent claim, read in light of the rest of the patent and its Patent Office file, must "reasonably  
9 apprise those skilled in the art" as to its scope; and, 2) the patent claim must be "as precise as  
10 the subject matter permits." *Amgen, Inc. v. Chugai Pharmaceutical Co.*, 927 F.2d 1200, 1217.  
11 (Fed. Cir. 1991), quoting *Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 624  
12 (Fed. Cir. 1985). InterTrust's patents fail both parts of the test, as demonstrated by both the  
13 intrinsic and extrinsic evidence.

14 2. "Secure" and Its Variants Are Indefinite Terms That Render the  
15 Claims Containing Them Invalid

16 The evidence is overwhelming that "secure" lacks a definite meaning in the art. It  
17 is a general term that both parties' experts and every third-party witness agree is vague unless  
18 given substantial context. InterTrust never provided the needed context in any part of its patents.  
19 Accordingly, persons of ordinary skill in the art cannot tell what "secure" means when reviewing  
20 the claims. "A claim term is indefinite if it can have more than one meaning to a person of  
21 ordinary skill in the art, and the appropriate meaning of the term is not explained in the  
22 specification" See *Union Pacific Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684, 692  
23 (Fed. Cir. 2001) (finding the term "comparing" indefinite); *In re Cohn*, 58 C.C.P.A. 996, 438 F.2d  
24 989, 993 (CCPA 1971) (finding claim term indefinite where the patentee's conflicting use of the  
25 term rendered the scope of the claims uncertain)." *VLT, Inc. v. Arterys Techs. Inc.*, 238 F. Supp.  
26 2d 339. Here, those of skill in the art, including InterTrust's own expert, have testified that secure  
27 can mean countless things to countless different people.

1 Although words of "degree" and other "relative" terms are sometimes upheld,  
2 "when a word of degree is used, the district court must determine whether the patent's  
3 specification provides some standard for measuring that degree." See *Seattle Box Company, Inc.*  
4 *v. Industrial Crating & Packaging, Inc.*, 731 F.2d 818, 826 (Fed. Cir. 1984). Here, as shown  
5 above, the specification not only fails to provide the necessary context, it adds to the ambiguity.  
6 Without some constraining parameters, subjective adjectives like "secure" are indefinite. A  
7 predecessor to the Federal Circuit, for example, affirmed the rejection of claims using the  
8 "relative" terms "stiff" and "resilient" (describing brush bristles) because the patent provided no  
9 guidance as to how stiff or how resilient. See *Application of Lechene*, 277 F.2d 173, 176  
10 (C.C.P.A. 1960). Stiff, unlike "secure," is one-dimensional – the only question was "how stiff?"  
11 "Secure" raises not only the question of "how secure," but also, "what kind of security," "from  
12 whom," and so on.

13 Moreover, InterTrust's indexing of "secure" to customer preferences in the  
14 specification makes it comparable to a rejected claim brought before the Board of Patent Appeals  
15 and Interferences in *Ex parte Brummer*, 12 USPQ2d (BNA) 1653 (BPAI 1989). In *Brummer*, the  
16 claim was directed to an improved recumbent bicycle having "a wheelbase that is between 58  
17 percent and 75 percent of the height of the rider that the bicycle was designed for." The Board  
18 held that "whether the bicycle was covered by the claim would be determined not on the basis of  
19 the structural elements and their interrelationships, as set forth in the claim, but by means of a  
20 label placed upon the bicycle at the discretion of the manufacturer." *Id* at \*\*3-4. The Board  
21 noted that with such claim language, a claim may be infringed when ridden by one rider, but not  
22 when ridden by another. Similarly, because the "level of security and tamper resistance required  
23 for trusted SPU hardware processes depends on the commercial requirements of particular  
24 markets or market niches, and may vary widely," (Ex. Q, '193 at 49:59-62), the scope of the  
25 claims depends on unpredictable, ill defined and ever-changing market factors. Indeed,  
26 InterTrust's use of "secure" is more indefinite than the language at issue in *Brummer*. In that  
27 case, the indefinite language allowed the patentee to vary the meaning of the claims as to one  
28 variable (size of the wheelbase); InterTrust's claims apparently seek leeway to shift and remold

1 themselves along all of the different axes of "security" discussed above.

2 Finally, secure and its variants further fail the definiteness requirement in failing to  
3 be as "precise as the subject matter allows." As demonstrated by its own documentation and by  
4 the widespread availability of model security policies, InterTrust had the ability to provide more  
5 definite meanings. It did not, and therefore the claim terms are not "as precise as the subject  
6 matter permits." *Amgen, Inc. v. Chugai Pharmaceutical Co.*, 927 F.2d 1200 at 1217.

7 Claim indefiniteness is particularly problematic where it derives from  
8 "conveniently functional language at the exact point of novelty." *General Electric Co. v. Wabash*  
9 *Appliance Corp.*, 304 U.S. 364, 371-372, 58 S. Ct. 899, 902-03 (1938). As InterTrust's own  
10 expert testified, "security" is an "essential aspect" of the alleged invention. Reiter Depo., at  
11 23:21-24:9. Accordingly, although no term should be ambiguous in a patent claim, it is  
12 particularly inexcusable that this "core" term be left hopelessly vague. *Exxon Research &*  
13 *Engineering Co. v. United States*, 265 F.3d 1371, 1379 (Fed. Cir. 2001) (fatal for limitations  
14 critical to patentability to be indefinite).

15 B. New Or Coined Terms Must Be Defined Or Otherwise Made Clear.

16 If the patentee elects to use "a term with no previous meaning to those of ordinary  
17 skill in the art ... [i]ts meaning ... must be found somewhere in the patent." *J.T. Eaton & Co. v.*  
18 *Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1568 (Fed. Cir. 1997) (emphasis added). In  
19 introducing the coined terms "protected processing environment" and "host processing  
20 environment," InterTrust had a "duty to provide a precise definition" for them. It failed to do so.  
21 Accordingly, these terms are indefinite and the claims containing them, invalid.

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

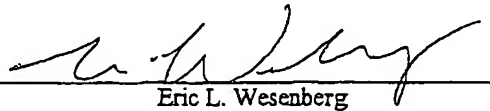
28 ///

1 IV. CONCLUSION

2 For the foregoing reasons, and those set forth in the accompanying Report and Declaration of  
3 Professor Mitchell, the Court should grant partial summary judgment that the following eleven  
4 claims are indefinite and invalid under 35 U.S.C. § 112, ¶ 2: claims 1, 11, and 15 of the '193  
5 patent; claim 2 of the U.S. Patent No. 6, 185,683; claims 1 and 34 of U.S. Patent No. 6,157,721;  
6 claim 58 of U.S. Patent No. 5, 920,861; claim 1 of U.S. Patent No. 5, 982,891; claim 155 of U.S.  
7 Patent No. 5,892,900; and claims 8 and 35 of U.S. Patent No. 5,917,912.

8 Dated: March 17, 2003

9 WILLIAM L. ANTHONY  
ERIC L. WESENBERG  
KENNETH J. HALPERN  
10 ORRICK, HERRINGTON & SUTCLIFFE LLP

11   
12 Eric L. Wesenberg

13 Attorneys for Defendant and Counterclaimant  
14 MICROSOFT CORPORATION  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28